Missouri Office of Information Technology

The Information Security Management Office (ISMO) Incident Response Plan and Procedures	**Document Number:** **ITGS0010**
	Effective Date: **12/19/2001**
	Published By: Office of Information Technology

1.0 Purpose

This document is intended to raise the awareness of the State's IT community of information security threats and concerns to minimize the damage from security incidents and malfunctions and to monitor and learn from them.

2.0 Scope

The incident response plan and procedures shall become the standard by which all State of Missouri information systems monitor and respond to security threats.

3.0 Background

As part of a comprehensive security program for the State, the Information Security Management Office (ISMO) in the Division of Information Services is implementing an Incident Response Plan and Procedures. It is imperative that the State's IT community is aware of information security threats and concerns to minimize the damage from security incidents and malfunctions and to monitor and learn from them.

4.0 References

4.1 ITAB Meeting Minutes:
December 19, 2001 http://oit.mo.gov/itab/minutes/ab_01_12.pdf

5.0 Revision History

Date	Description of Change
12/19/2001	Initial Plan and Procedures Published

6.0 Definitions

Incident An adverse event, or threat of an adverse event, in a computer system and/or network

7.0 Inquiries

Direct inquiries about this document to:

Office of Information Technology
Truman Building, Room 560
301 W. High Street
Jefferson City, MO 65102
Voice: 573-526-7741
FAX: 573-526-7747

Parts of this document are exempt from public disclosure based on RSMo Chapter 610, Section 610.021 Sub-Paragraph (20) which states:

610.021 Except to the extent disclosure is otherwise required by law, a public governmental body is authorized to close meetings, records and votes, to the extent they relate to the following:

(20) Records that identify the configuration of components or the operation of a computer, computer system, computer network, or telecommunications network, and would allow unauthorized access to or unlawful disruption of a computer, computer system, computer network, or telecommunications network of a public governmental body.

Page down to view the public version of this document

Incident Response Plan and Procedures

As part of a comprehensive security program for the State, the Information Security Management Office (ISMO) in the Division of Information Services is implementing an Incident Response Plan and Procedures. It is imperative that the State's IT community is aware of information security threats and concerns to minimize the damage from security incidents and malfunctions and to monitor and learn from them.

The term "incident" refers to an adverse event, or threat of an adverse event, in a computer system and/or network.

1. Types of incidents and when to report.

What type of incident must I report?

- Successful attempts to gain unauthorized access to systems or data;
- Unwanted disruption or denial of service;
- The unauthorized use/access of a system for the transmission, processing or storage of data;
- Changes to system hardware, firmware, and/or usage of software characteristics without the owner's knowledge, instruction or consent.
- Discovery of malicious code to include worms, viruses, Trojans, or web defacement, etc.
- Any breach of the computing environment that has the potential to spread outside of the agency's immediate control.

At the discretion of the agency CIO/IT Director, impacts to the computing environment that are contained within the agency's system and will not have an adverse impact on other agencies are not required to be reported. (i.e....pings/scans)

When should I report an incident?

Report any incident immediately that meets the above definition and criteria or is suspicious in nature. We encourage primary or secondary contacts for ITAB member agencies to report all suspicious activity, even if the incident is quite old at the time of reporting. Incident reports that are sent shortly after the incident occurred are the most likely to be of value. This does not imply that an incident report becomes useless after some period of time. Remember a report not only is the first step in recovery but it also helps raise awareness and contributes to the overall information security posture of the enterprise.

2. How to report and what should be included

- How to report an incident?
  Primary or secondary contacts for ITAB member agencies report and/or route incidents to the Technology Services help desk.
- What should I include in the incident report?
  When reporting an incident, it is important to ensure that you provide enough information for our Information Security Management Office (ISMO) staff to be able to understand and respond efficiently and effectively.
- Please supply the following:

- Contact information (who to contact for followup information)
- Location information (where is the problem taking place)
- Host/networks involved (how many systems/networks are affected)
- Attack description (what is/has happened)
- Impact (SEV1, SEV2, SEV3) (if applicable)

Severity levels:

o SEV1 = network/system totally down,
o SEV2 = network/system is 50% viable,
o SEV3 = spot outages

- For the development of preventative measures and reporting of the incident to the appropriate enforcement organizations a detailed report of the incident will be developed.

3. What will the Helpdesk do?

Technology Services help desk will take reported incidents from the "Contact Information for Virus/Security Incident Coordination" list. Only those reports verified by those listed as contacts will be considered as valid. Additionally, the help desk will log the incident report, assign a ticket number (as per the TS Customer Procedures Manual) and will immediately forward the report to ISMO staff for handling.

4. ISMO staff notifies appropriate agencies

The process begins with ISMO staff recording an "alert" message into a special voice mailbox, which is the security services incident reporting mailbox. ISMO staff will then instruct the Technology Services helpdesk to activate the incident notification procedure. ISMO staff will then send a message to the voice mailboxes of the ITAB member agency primary and secondary contacts.

Note: This system automatically calls each ITAB member agency primary and secondary contacts.

The message will be marked "return receipt" so the system can automatically notify ISMO staff which contacts have not played the message. The voice message will also be marked "urgent" so that it will be the first message in each mailbox.

The second step in the process will prompt the called party to contact their state voice mailbox or call the incident reporting mailbox. If the system calls a pager it leaves an alpha-numeric message to call voice mail for details. If the system calls a third party or an answering machine a message will be played instructing the ITAB member agency primary and secondary contacts to call voice mail. If the primary or secondary contact answers the call the system will prompt the contact to verify message receipt by pressing a special code on the dialpad. In case of a busy signal or no answer the system will repeat the notification process.

ISMO staff will continue to monitor the problem and update the voicemail message and distribute the updates to the ITAB member agency primary and secondary contact mailboxes as the status changes. This process will essentially create an event log with time and date stamped voice message status reports.

The notification process will conclude with an end of alert message.

5. ISMO staff performs an initial incident analysis
The initial incident analysis will include:

Collecting evidence

- impact statements from affected customers, including descriptions of the "threat" manifestations and other network or system behaviors.
- incident and activity logs, application and system logs,
- isolated examples of the virus(es) or worm(s),
- anecdotal information.

Develop timelines

- Establish incident timeline. Identify each significant event or behavior associated with the incident from the report and place on the timeline. Pick the earliest date known of the incident to establish emergence. This does not necessarily establish the Incident Reporting date as the genesis. An

anecdotal report of a date preceding the incident does not preempt the Incident Report date, but adds to the body of knowledge.
- Establish common thread and modes of behaviors from examining the time line and other reports derived from empirical query of the Incident Reporting database.

Evaluate impact from customers.

- Percent of system/network outage (estimated) and assigned severity levels of 1,2,3.
- Evaluate and or determine threat entry point to systems affected and list vulnerabilities.
- Perform computer and network forensics, including information distilled from the evidence, the assessment of remedies, dissemination of those remedies, and preventive measures
- Transmit a notification to the affected customers immediately, if the vulnerabilities are clearly fatal to the continued operations of the affected customers or puts the entire State of Missouri Enterprise at risk.

NOTE: Customer should add any new vulnerabilities discovered during this time to the list.

6. Assess remedies and disseminate

Upon the initial notification of the incident to the ISMO staff, empirical data will be used to assist in identifying the threat, its severity and bring remedy. In cases involving viruses and worms, anti-virus vendor services will be employed to provide threat eradication.

ISMO staff will provide a list of effects of the threat eradication.

7. Develop preventative measures

ISMO staff will continue to develop preventive measures by further assessment of incident analysis data using a post-mortem protocol with a list of questions designed to populate an online survey instrument. Once the results are summarized, a preventive plan is created and posted on a web site/page for the customer. A preventive plan will include, listing of training and education, how to bring about elimination of the vulnerabilities, etc.